

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347942

(43)Date of publication of application : 15.12.2000

(51)Int.Cl.

G06F 12/14

G06F 11/22

G06F 15/78

(21)Application number : 11-158256

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 04.06.1999

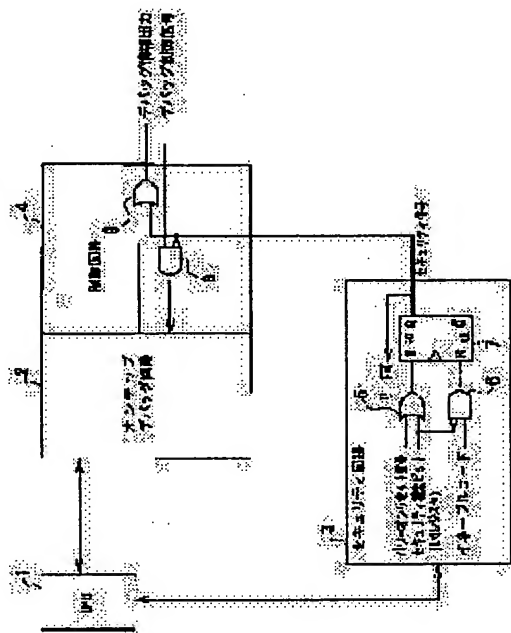
(72)Inventor : TANABE TETSUYA
ASAI EIICHI

(54) INFORMATION PROCESSOR

(57)Abstract:

PROBLEM TO BE SOLVED: To protect information stored in a ROM from an illegal access caused by a debug tool provided externally.

SOLUTION: An on-chip debug circuit 2 mounted in the information processor is made invalid by power-on reset, and an on-chip debug ICE(in-circuit emulator) is prohibited from accessing an incorporated ROM. The invalidation of the circuit 2 is released by setting an I/O register released to a user by a user program.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-347942

(P2000-347942A)

(43) 公開日 平成12年12月15日 (2000. 12. 15)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 E 5 B 0 1 7
11/22	3 4 0	11/22	3 4 0 A 5 B 0 4 8
15/78	5 1 0	15/78	5 1 0 C 5 B 0 6 2

審査請求 未請求 請求項の数 5 O L (全 8 頁)

(21) 出願番号 特願平11-158256

(22) 出願日 平成11年6月4日 (1999. 6. 4)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 田部 徹也

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝マイクロエレクトロニクスセンター内

(72) 発明者 浅井 栄一

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝マイクロエレクトロニクスセンター内

(74) 代理人 100083806

弁理士 三好 秀和 (外7名)

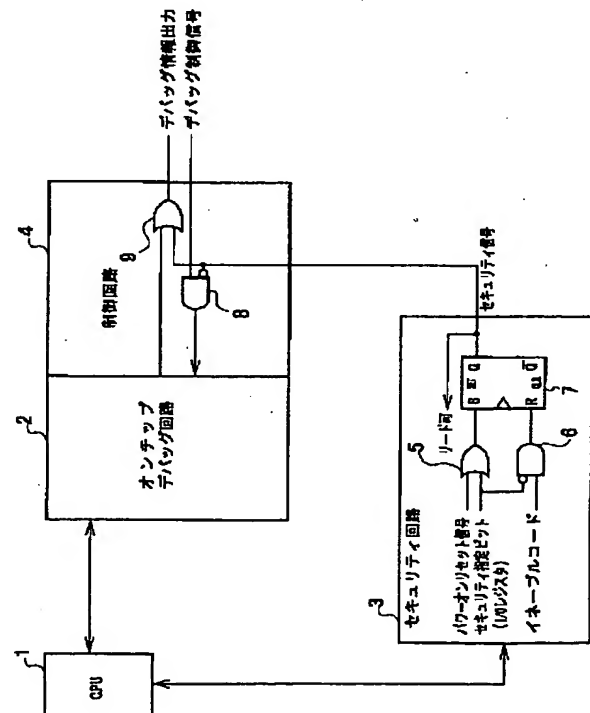
最終頁に続く

(54) 【発明の名称】 情報処理装置

(57) 【要約】

【課題】 この発明は、ROMに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することを課題とする。

【解決手段】 この発明は、情報処理装置内に実装されているオンチップデバッグ回路2をパワーオンリセットにより無効化し、オンチップデバッグICEによる内蔵ROMのアクセスを禁止し、オンチップデバッグ回路の無効化は、ユーザプログラムによりユーザに開放されたI/Oレジスタの設定により解除されるように構成される。



(2)

【特許請求の範囲】

【請求項1】 ユーザにより個別に設定可能なユーザプログラムからなるセキュリティ解除プログラムを記憶情報に含み、外部に設けられたエミュレータによる不正アクセスから保護する情報を記憶するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力制御を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化してセキュリティを設定し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、セキュリティ指定ビットと、このセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードとを受けて、前記オンチップデバッグ回路の機能を有効化してセキュリティを解除し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする情報処理装置。

【請求項2】 前記セキュリティ指定ビットは、電源投入時にセットされて前記オンチップデバッグ回路の機能が無効化されセキュリティが設定されている状態、又は前記ROMに記憶されたセキュリティ解除プログラムによりリセットされて前記オンチップデバッグ回路の機能が有効化されセキュリティが解除されている状態を有することを特徴とする請求項1記載の情報処理装置。

【請求項3】 前記セキュリティ回路は、前記オンチップデバッグ回路を無効化する際に、一部機能を有効化してなることを特徴とする請求項1記載の情報処理装置。

【請求項4】 外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードとを照合して両者が一致した場合には、前記オンチップデバッグ回路の機能を有効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする情報処理装置。

【請求項5】 外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、

前記エミュレータから暗号化されて前記情報処理装置に与えられるデバッグに必要な信号を復号化し、前記情報処理装置のデバッグ結果を暗号化して前記エミュレータに出力する暗号化回路とを有することを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、外部に設けられたオンチップデバッグICEに接続されてデバッグをサポートするオンチップデバッグ回路を備え、オンチップデバッグICEによるデバッグ時に内蔵ROMのデータを不正アクセスから保護する情報処理装置に関する。

【0002】

【従来の技術】従来、図3に示すように、オンチップデバッグ回路100を備えたマイコン101等の情報処理装置においては、外部にオンチップデバッグICE（インサーキットエミュレータ）102を接続することにより、オンチップデバッグICE102を用いてブレーク、トレース、モニタなどのエミュレータ機能が使用できるようになる。これにより、マイコン101内の機能の参照やプログラムの実行軌跡を解析でき、プログラムの開発、デバッグや故障解析が可能となる。

【0003】しかし、このオンチップデバッグICE102を使用することにより、例えばマイコン101の内蔵ROM103に記憶されていた情報がマイコン101の外部に容易に読み出すことが可能となっていた。これにより、特定のユーザ以外の不特定のユーザであってもマイコン101内のプログラムの参照や解析が可能になっていた。

【0004】

【発明が解決しようとする課題】以上説明したように、デバッグをサポートするオンチップデバッグ回路を備えた従来の情報処理装置にあっては、外部に用意されたオンチップデバッグICEをオンチップデバッグ回路に接続することにより、誰でも情報処理装置内の情報を容易に外部に取り出すことが可能となっていた。このため、装置内のROMに記憶されたプログラム等の情報を不正アクセスから保護することが困難になるといった不具合を招いていた。

【0005】そこで、この発明は、上記に鑑みてなされたものであり、その目的とするところは、ROMに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することができる情報処理装置を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するために、課題を解決する第1の手段は、ユーザにより個別に設定可能なユーザプログラムからなるセキュリティ解除プログラムを記憶情報に含み、外部に設けられたエミュレータによる不正アクセスから保護する情報を記憶する

3

メモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力制御を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化してセキュリティを設定し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、セキュリティ指定ビットと、このセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードとを受けて、前記オンチップデバッグ回路の機能を有効化してセキュリティを解除し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする。

【0007】第2の手段は、前記第1の手段において、前記セキュリティ指定ビットは、電源投入時にセットされて前記オンチップデバッグ回路の機能が無効化されセキュリティが設定されている状態、又は前記ROMに記憶されたセキュリティ解除プログラムによりリセットされて前記オンチップデバッグ回路の機能が有効化されセキュリティが解除されている状態を有することを特徴とする。

【0008】第3の手段は、前記第1の手段において、前記セキュリティ回路は、前記オンチップデバッグ回路を無効化する際に、一部機能を有効化してなることを特徴とする。

【0009】第4の手段は、外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードとを照合して両者が一致した場合には、前記オンチップデバッグ回路の機能を有効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする。

【0010】第5の手段は、外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、前記エミュレータから暗号化されて前記情報処理装置に与えられるデバッグに必要な信号を復号化し、前記情報処理装置のデバッグ結果を暗号化して前記エミュレータに出力する暗号化回路とを有することを特徴とする。

(3)

4

【0011】

【発明の実施の形態】以下、図面を用いて本発明の実施形態を説明する。

【0012】図1はこの発明の一実施形態に係る情報処理装置の要部構成を示す図であり、図2はデバッグの手順を示すフローチャートである。

【0013】図1において、この実施形態の情報処理装置のマイコンは、CPU1、図示しないROMや周辺回路に加えて、前述したと同様のオンチップデバッグ回路2、セキュリティ回路3、制御回路4を備えて構成されている。

【0014】セキュリティ回路3は、電源投入時にマイコンをリセットするパワーオンリセット信号とセキュリティ指定ビットを入力とする論理和（OR）ゲート5と、セキュリティ指定ビットの反転とセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードを入力とする論理積（AND）ゲート6と、ORゲート5の出力をセット（S）入力としANDゲート6の出力をリセット（R）入力とし出力（Q）をセキュリティ信号として制御回路4に与えるレジスタ（RSフリップフロップ）7を備え、パワーオンリセット信号を受けてオンチップデバッグ回路2の機能を無効化してセキュリティを設定し、エミュレータによるメモリの記憶情報の読み出し、特にオンチップデバッグICE（インサーキットエミュレータ）によるROMの記憶情報の読み出しを禁止し、リセットされたセキュリティ指定ビットかつイネーブルコードを受けて、オンチップデバッグ回路2の機能を有効化してセキュリティを解除し、オンチップデバッグICEによるROMの記憶情報の読み出しを可能にする。

【0015】制御回路4は、セキュリティ回路3から与えられるセキュリティ信号の反転と、オンチップデバッグICEから与えられてマイコンをデバッグするのに必要となる信号のデバッグ制御信号を入力するANDゲート8と、セキュリティ信号とオンチップデバッグ回路2から与えられるデバッグ結果を入力としデバッグ情報出力をオンチップデバッグICEに出力するORゲート9を備え、セキュリティ信号がセキュリティ回路3から与えられてセキュリティが設定されている場合には、デバッグ制御信号の入力ならびにデバッグ情報の出力を禁止する。

【0016】次に、この実施形態では、以下のような方式でマイコン内のオンチップデバッグ回路2の動作を制御する。

【0017】セキュリティ用のセキュリティ指定ビットをI/Oレジスタに設ける。このセキュリティ指定ビットは、パワーオン時に“1”（セキュリティ有効）にセットされ、オンチップデバッグ回路2は、パワーオンリセットによってオンチップデバッグ回路2の機能が無効となるように初期化される。外部に接続されるオンチッ

(4)

5

デバッグICEからのデバッグリセット信号、デバッグ用割込み信号、デバッグ用制御プログラム入力信号のデバッグに必要な信号は無効となる。オンチップデバッグ回路2からオンチップデバッグICEへ出力されるデバッグ情報信号やオンチップデバッグICEとの同期クロックなども固定信号レベルとなり禁止される。

【0018】セキュリティの解除は、ユーザによって作成されてROMに格納されたユーザプログラムのセキュリティ解除プログラムにより行われ、セキュリティ指定ビットに“0”を書き込むとともにユーザI/Oレジスタのセキュリティクリアレジスタにイネーブルコードを書き込む。このように、セキュリティの解除は、二重設定により暴走による誤解除を防ぐことができる。

【0019】セキュリティの設定(ON)/解除(OFF)のステータスは、以下に示すようにして検知される。セキュリティON(セキュリティ有効)の状態検知は、セキュリティ指定ビットを読み出すと、“1”が読み出される。また、オンチップデバッグ回路2からオンチップデバッグICEへ出力されるデバッグ情報出力がすべて固定信号レベルとなっている。セキュリティOFF(セキュリティ解除)の状態検知は、セキュリティ指定ビットを読み出すと、“0”が読み出される。また、オンチップデバッグ回路2からオンチップデバッグICEへデバッグ情報出力と、オンチップデバッグICEとの同期クロックが出力される。

【0020】オンチップデバッグICEへの制限事項として、セキュリティ機能が解除されるまで、オンチップデバッグICEは使用できない。マイコン内のオンチップデバッグ回路2はオンチップデバッグICEからのデバッグリセットやブレーク要求に無反応であり、オンチップデバッグICEに対するデバッグ情報出力も常に固定レベルとなる。この制限は、パワーオン時のみ起こり、セキュリティ解除後は、ユーザリセットやオンチップデバッグICEからのリセットによって再びセキュリティON(有効)になることはない。

【0021】次に、想定されるユーザの使用例を図2のフローチャートを参照して説明する。

【0022】プログラム開発やメンテナンスのためにオンチップデバッグICEを使用するユーザ(正規ユーザ)の場合に、オンチップデバッグICEをマイコンに接続し、ターゲットシステムのマイコンとオンチップデバッグICEを立ち上げた時、オンチップデバッグICEはデバッグリセットをマイコンに要求するが(図2(ステップS1))、オンチップデバッグ回路2はパワーオンリセットにより禁止されているため、このリセットは受け付けられない(図2(ステップS2))。また、デバッグ情報出力が固定レベルとなっていることからエラーメッセージをオンチップデバッグICEは出力する。もしくは、マイコンからの反応がないため、オンチップデバッグICEも無反応状態となる。

6

【0023】次に、ターゲットシステムとターゲットプログラムによりセキュリティが解除されオンチップデバッグが許可される場合に、ユーザがそれぞれ独自に作成したターゲットプログラム中のセキュリティ判定ルーチンにより、セキュリティ解除許可と判断された場合には(図2(ステップS3, S4))、マイコンのセキュリティI/Oレジスタへの書き込みルーチンの実行が同じくユーザプログラムにより行われ、オンチップデバッグ回路2は許可状態になる。この判定ルーチンでは、ターゲットシステムのスイッチの状態など、外部からの信号も使用される場合がある。オンチップデバッグ回路2の許可により、デバッグ情報やオンチップデバッグICEとの同期クロックが出力される(図2(ステップS5))。

【0024】マイコンは、オンチップデバッグICEからのリセットによりデバッグリセットが発生する。これにより、オンチップデバッグICEの動作も可能となり、この後はオンチップデバッグICEが立ち上がり、モニタプログラムが動作し、ユーザプログラムの実行が要求される(図2(ステップS6, S7))。この後、リセットが発生してもセキュリティはオフでオンチップデバッグは許可のままとなる。パワーオフとなるまでオンチップデバッグICEが使用可能となる。

【0025】一方、オンチップデバッグICEを使用して、内蔵ROMの内容を不正にアクセスしようとするユーザ(不正規ユーザ)の場合には、オンチップデバッグICEを接続し、ターゲットとオンチップデバッグICEを立ち上げる。この時、オンチップデバッグICEはデバッグリセットをマイコンに要求するが(図2(ステップS1))、オンチップデバッグ回路2はパワーオンリセットにより禁止されているため、このリセットは受け付けられない。また、デバッグ情報出力が固定レベルとなっていることからエラーメッセージをオンチップデバッグICEは出力する。もしくはマイコンからのレスポンスがないため、オンチップデバッグICEも無反応状態となる。

【0026】次に、セキュリティがON(有効)のままターゲットプログラムを実行する。しかし、不正規ユーザはセキュリティ解除の方法がわからないため、正規ユーザが独自に作成したターゲットプログラム中のセキュリティ判定ルーチンにより、セキュリティ許可とはならない。したがって、ユーザプログラムは実行可能であるが、オンチップデバッグICEはエラー出力、もしくは無反応状態が続く。

【0027】このように、上記実施形態にあつては、マイコン内のROMに書かれたプログラム情報が不正にアクセスしようとするユーザに開示されず守秘が保たれる。また、セキュリティ解除プログラムをユーザが自由に書けるため、セキュリティ解除の方法が無限となり、守秘性が高い。さらに、セキュリティ制御にパワー

(5)

7

オンリセットを利用することにより、一度セキュリティが解除された後は、マイコンの電源を落とすまで、制限無くオンチップデバッグICEを使用できる。

【0028】次に、この発明の他の実施形態について説明する。

【0029】この実施形態の特徴とするところは、上記実施形態のセキュリティ解除判定ルーチンにおいて、予めマイコン内に設定したコードと、外部入力やオンチップデバッグICEからの入力を比較して判定するパスワード方式としてセキュリティの解除プログラムを作成せず、図1に示すセキュリティ回路3に代えて、パワーオンリセット信号によりオンチップデバッグ回路2の機能を無効化し、オンチップデバッグICEによるROMの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードを照合して両者が一致した場合には、オンチップデバッグ回路2の機能を有効化し、オンチップデバッグICEによるROMの記憶情報の読み出しを可能にする、パスワード判定回路を含むセキュリティ解除回路を組み込む構成を採用したことにある。このような実施形態にあっても、上記実施形態と同様な効果を得ることができる。

【0030】次に、この発明の他の実施形態について説明する。

【0031】この実施形態の特徴とするところは、前述した図1に示す実施形態でのセキュリティ有効時に、オンチップデバッグ機能のすべてを禁止するのではなく、一部のデバッグ機能を許可する、例えばユーザアプリケーションにおいて使用するデバッグ機能があれば、その部分のみ常時許可するようにしたことにある。

【0032】一方、オンチップデバッグICEから暗号化されて情報処理装置に与えられるデバッグに必要な信号を復号化し、情報処理装置のデバッグ結果を暗号化してオンチップデバッグICEに出力する暗号化回路を設け、セキュリティ有効時に、デバッグ情報を暗号化してオンチップデバッグICEへ出力し、オンチップデバ

8

グICE側でその暗号の解読を制御し、正規ユーザーのみ暗号を解読してデバッグできるようにしてもよい。このような実施形態にあっても、上記実施形態と同様な効果を得ることができる。

【0033】

【発明の効果】以上説明したように、この発明によれば、パワーオンリセットにより情報処理装置内に実装されているオンチップデバッグ回路を無効化しセキュリティを設定し、オンチップデバッグICEによる内蔵ROMのアクセスを禁止し、ユーザプログラムにより設定制御されるセキュリティ指定ビットに基づいてセキュリティが解除されるようにしたので、ROMに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することが可能となる。また、セキュリティの解除方法は、ユーザが自由に設定できるため、セキュリティの解除方法が無限となり、守秘性が高くなる。さらに、セキュリティの制御にパワーオンリセットを利用することにより、一度セキュリティが解除された後は、電源がオフされるまでオンチップデバッグICEを制限なく使用することができる。

【図面の簡単な説明】

【図1】この発明の一実施形態に係る情報処理装置の要部構成を示す図である。

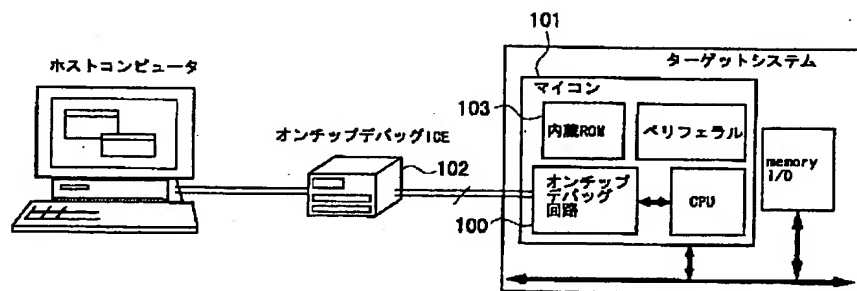
【図2】図1に示す実施形態の動作手順を示すフローチャートである。

【図3】ターゲットシステムをデバッグする従来のシステムを示す図である。

【符号の説明】

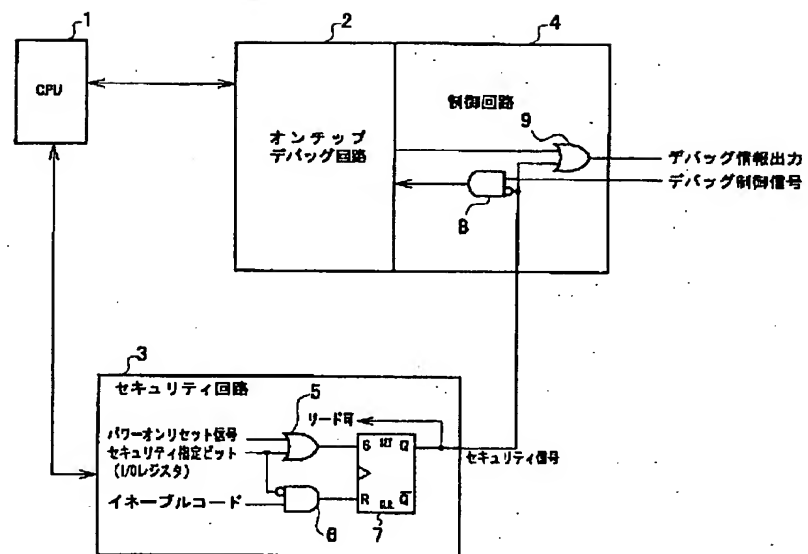
- 1 CPU
- 2 オンチップデバッグ回路
- 3 セキュリティ回路
- 4 制御回路
- 5, 6, 8, 9 論理ゲート
- 7 レジスタ

【図3】



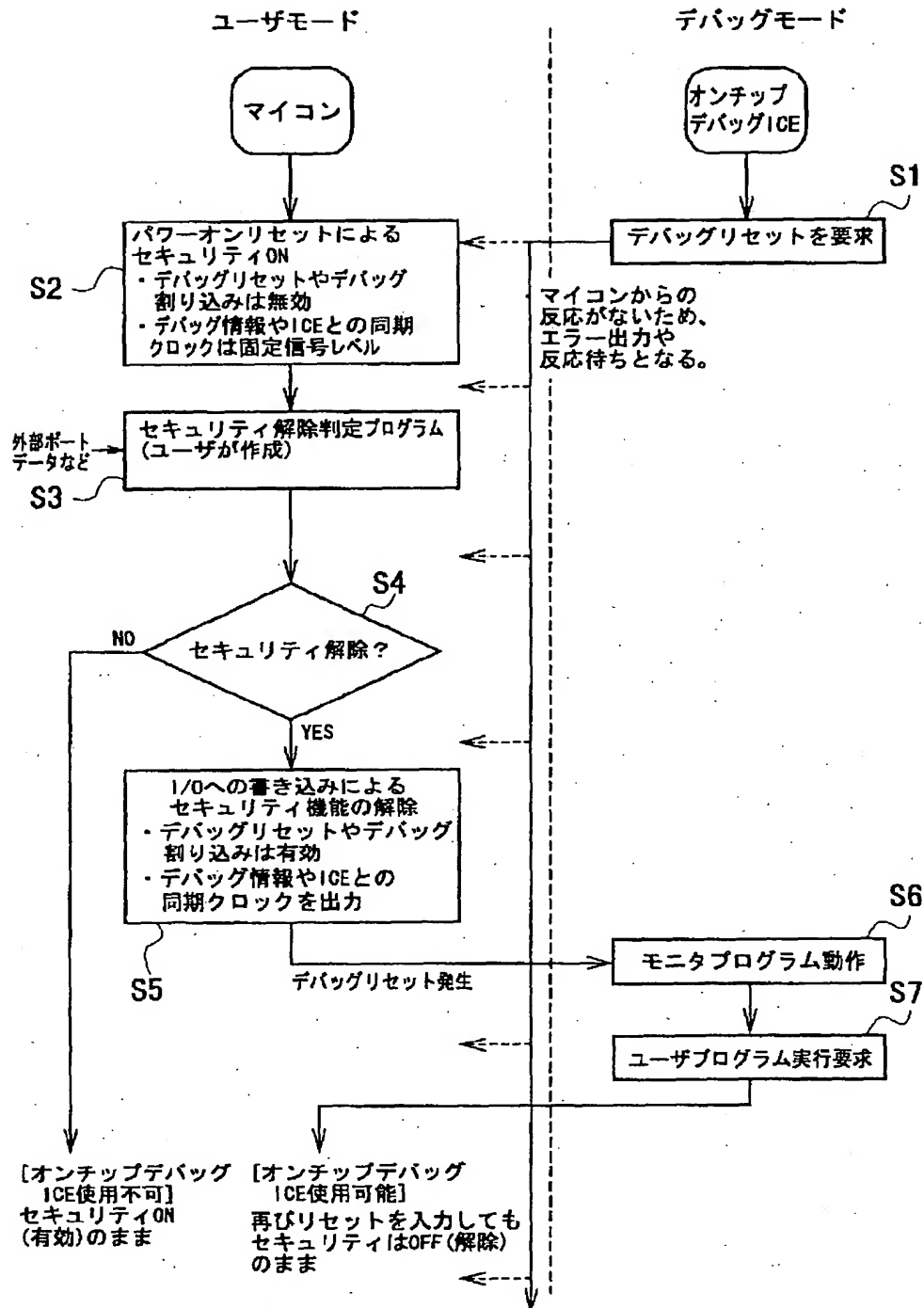
(6)

【図1】



(7)

【図 2】



(8)

フロントページの続き

Fターム(参考) 5B017 AA01 BA05 BA07 BB03 BB05

CA12 CA16

5B048 AA19 BB02 CC05

5B062 AA07 DD10 GG05 HH09 JJ08